

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-313640

(43)Date of publication of application : 09.11.2001

(51)Int.Cl.

H04L 12/24  
H04L 12/26  
G06F 13/00  
H04L 12/22

(21)Application number : 2000-133494

(71)Applicant : NTT DATA CORP

(22)Date of filing : 02.05.2000

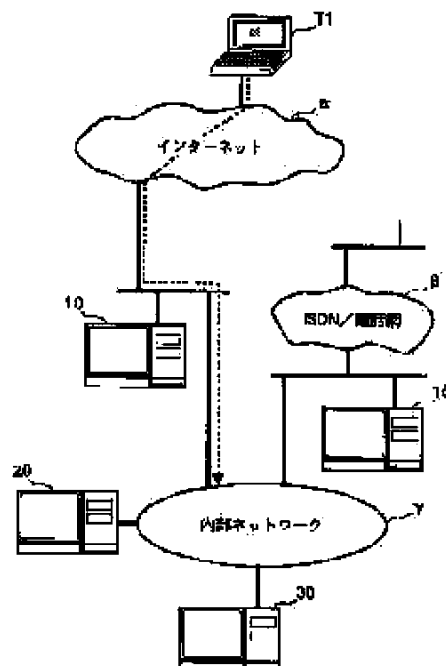
(72)Inventor : BABA TATSUYA  
YAMAOKA MASATERU  
KOKUBO KATSUTOSHI  
MATSUDA YOSHIYUKI

## (54) METHOD AND SYSTEM FOR DECIDING ACCESS TYPE IN COMMUNICATION NETWORK AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an illegal access detection system capable of detecting illegal accesses of various patterns including an unknown method.

SOLUTION: The latest access policy of a site to be a management object is acquired from a management server 20 and held. Packets addressed to the site are acquired among packets circulated in a network, and packets suitable for the access policy and packets unsuitable for the access policy are sorted amount the acquired packets. When a packet unsuitable for the policy is selected, the packet is specified as a packet having possibility of being an illegal access and notified to the management server 20 in order to change an access condition for removing an access based on the specified packet.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2001-313640  
(P2001-313640A)

(43) 公開日 平成13年11月9日 (2001.11.9)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テ-リ-ト <sup>*</sup> (参考)
H 0 4 L 12/24		G 0 6 F 13/00	3 5 1 Z 5 B 0 8 9
12/26		H 0 4 L 11/08	5 K 0 3 0
G 0 6 F 13/00	3 5 1	11/26	9 A 0 0 1
H 0 4 L 12/22			

審査請求 未請求 請求項の数5 O L (全 11 頁)

(21) 出願番号 特願2000-133494(P2000-133494)

(22) 出願日 平成12年5月2日 (2000.5.2)

特許法第30条第1項適用申請有り 平成12年3月14日～  
3月16日 社団法人情報処理学会主催の「第60回 (平成  
12年前期) 全国大会」において文書をもって発表

(71) 出願人 000102728

株式会社エヌ・ティ・ティ・データ  
東京都江東区豊洲三丁目3番3号

(72) 発明者 扇場 達也

東京都江東区豊洲三丁目3番3号 株式会  
社エヌ・ティ・ティ・データ内

(72) 発明者 山岡 正輝

東京都江東区豊洲三丁目3番3号 株式会  
社エヌ・ティ・ティ・データ内

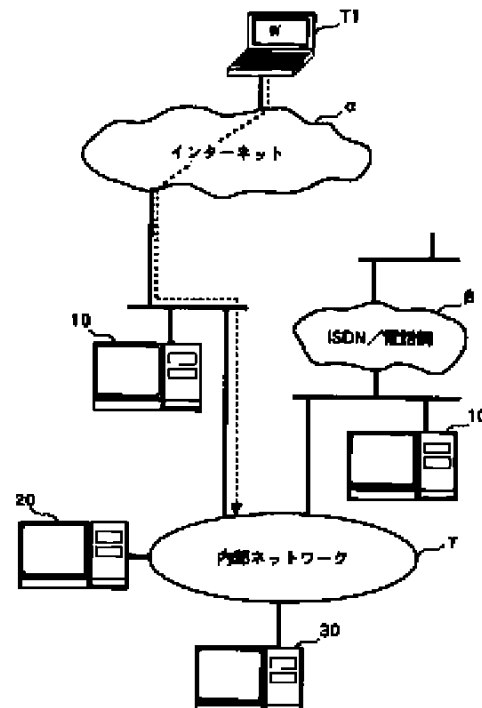
(74) 代理人 100099324

弁理士 鈴木 正剛

最終頁に続く

(54) 【発明の名称】 通信ネットワークにおけるアクセス種別を判定する方法及びシステム、記録媒体

(57)



(2)

*I*

*2*

*10*

*20*

*30*

*40*

*50*

*2*

P.A. Porras and P.G. Neumann. EMERALD: Event monitoring enabling responses to anomalous live disturbances. In Proceedings of the 20th National Information Systems Security Conference. pp. 353-365. Oct. 1997

10

20

Cisco Systems, Inc. Cisco Secure Intrusion Detection System  
Cisco Systems, Inc. RealSecure Internet Security

30

H.S. Javits and A. Valdes. The SRI IDES Statistical Anomaly Detector. In Proceedings of the IEEE Symposium on Security and Privacy, May 1991

IDS M OFS99 15 A199 27 pp 39  
46 July 1999

www world wide web DNS domain name service  
40

50

(4)

5

6

10

20

30

40

50

4

10

20

30

ISDN

MAC Media Access Contro

I

40

File Transfer Protocol

50

(6)

9

10

10

IP TCP UDP ICMP  
HTTP FTP SMTP DNS TELNET

20

IP  
TCP UDP ICMP  
HTTP SMTP DNS

30

IP

40

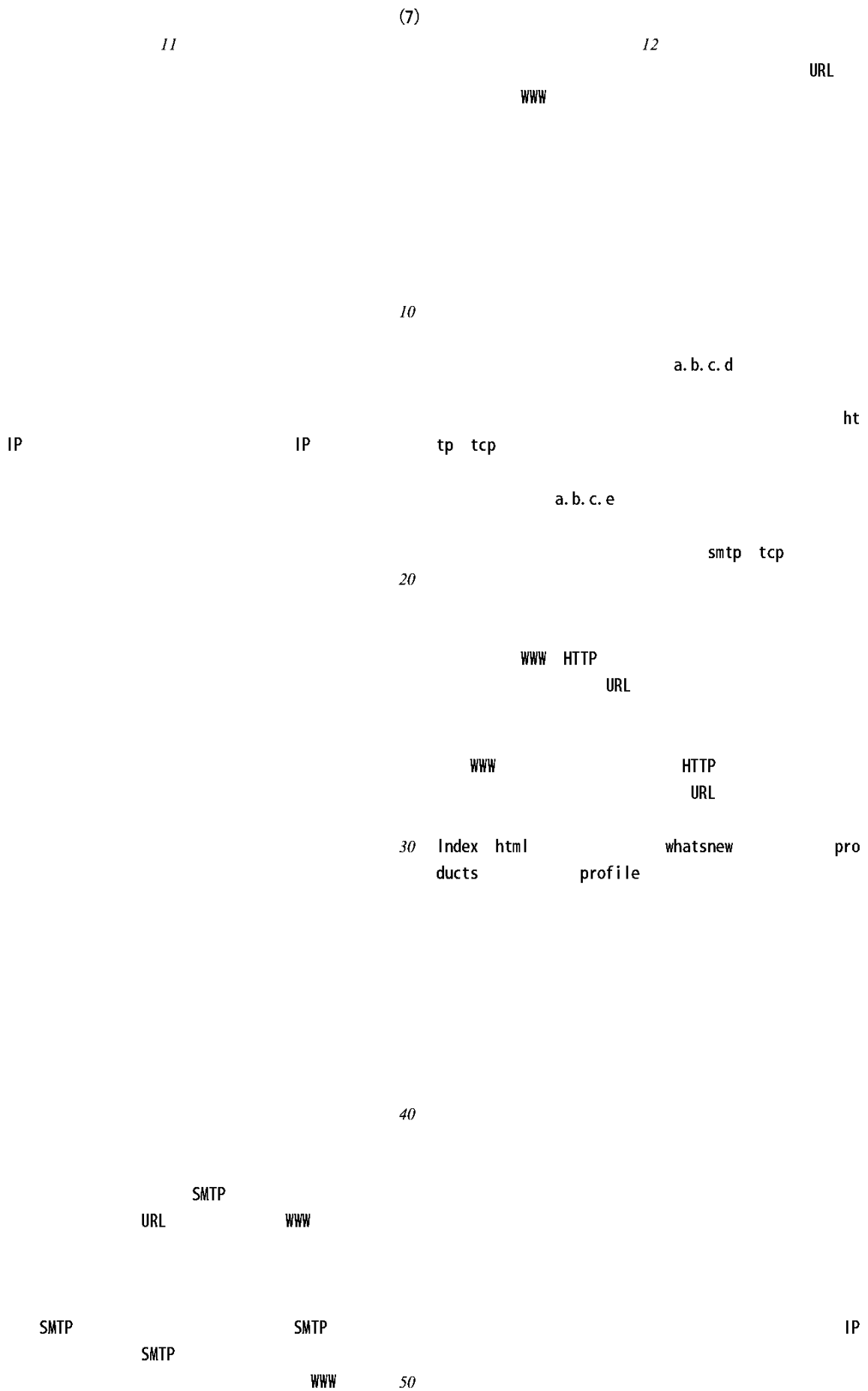
HTTP URL SMTP

File Transfe

r Protocol

50

6





(8)

13

14

HTTP  
P HTTP HTTP IP TC  
Yes  
IP  
IP  
IP

TCP IP HTT 10  
P

HTTP

HTTP  
RFC1945 RFC2068

HTTP

GE

T POST  
GET Request URL HTTP 1.1 1.1  
20  
GET Request URL HTTP 1.0 1.0

GET Request URL  
Request URL  
URL

HTTP 1.0 HTTP 1.1

30

TCP UDP

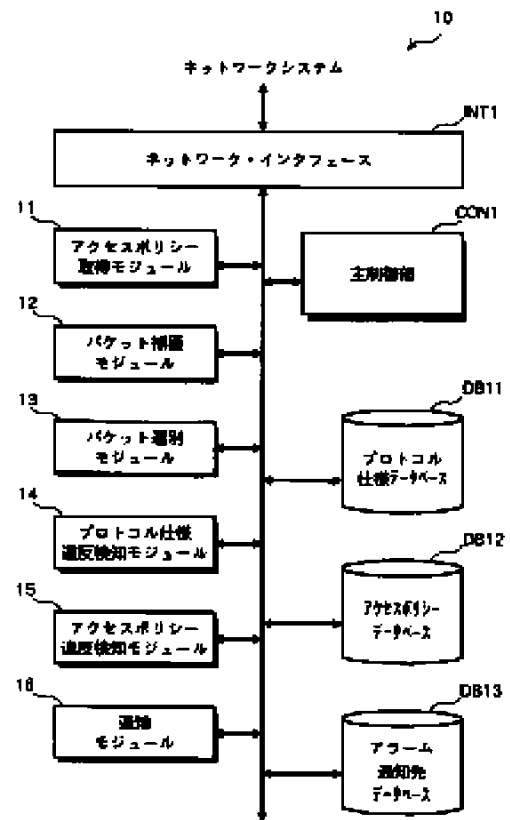
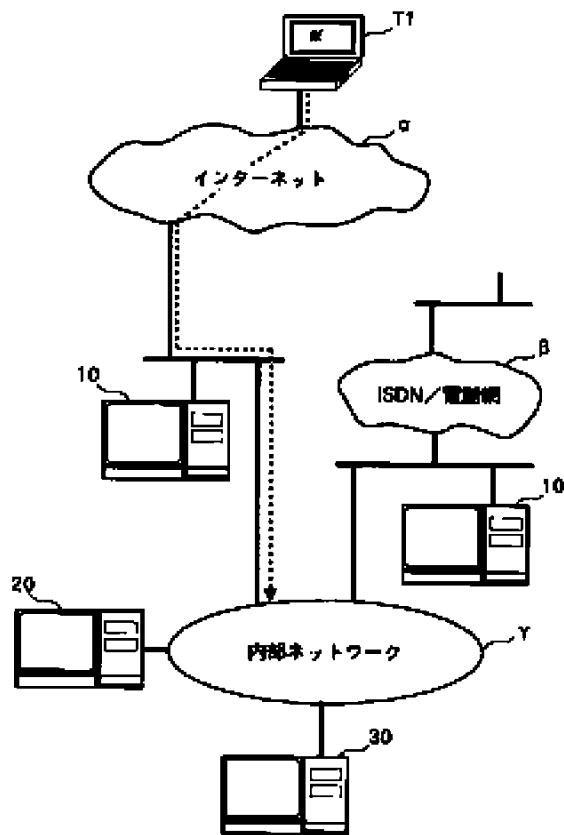
"Req

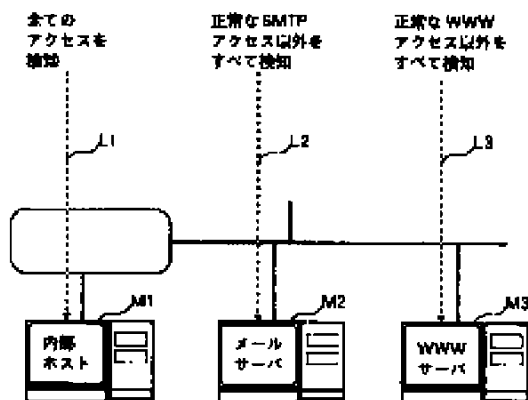
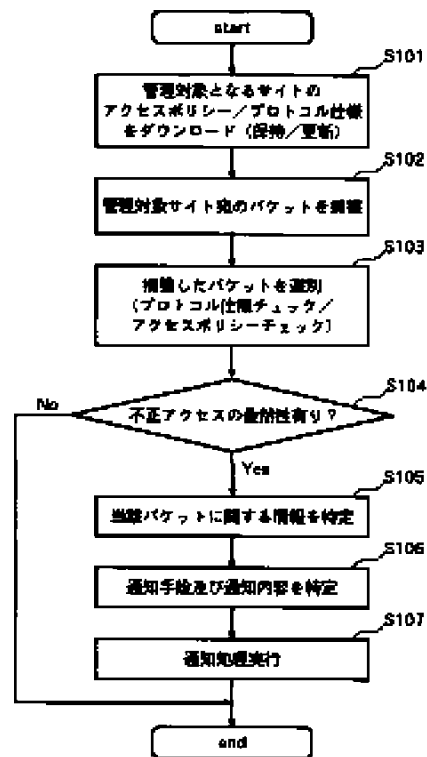
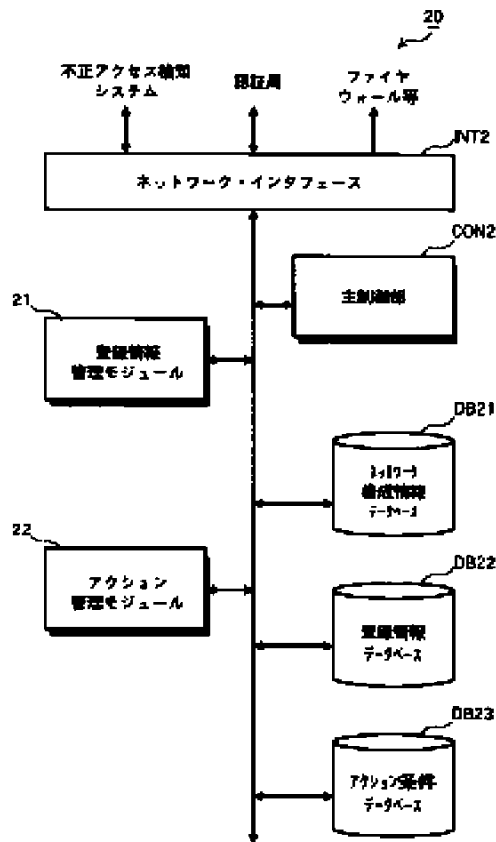
uest-URL"

40

No

50





送信元アドレス	宛先アドレス	プロトコル	ユーザ名	プロトコル特有の条件
すべて	a.b.c.d	http/tcp	ANY	公開するファイル /index.html /whatsnew/4 /profile/6 .....
すべて	a.d.e.e	smtp/tcp	ANY	使用するドメイン @11111111.co.jp @22222222.co.jp 許可するコマンド VRFY, EXPN

IPヘッダ	TCPヘッダ	HTTPヘッダ	HTTPデータ
-------	--------	---------	---------

(11)

通知手段	通知先	通知内容	使用
電子メール	postmaster@a.co.jp	不正アクセスが発生しました 送信先：宛先：プロトコル：	○
ポケベル	03-1234-5678	不正アクセスが発生しました 送信先：宛先：プロトコル：	×
コピー機		不正アクセスが発生しました 送信先：宛先：プロトコル：	○
---	-----	-----	

(a)

プロトコル仕様違反検知モジュール	チェック項目	チェック結果
I P	IPヘッダ長	正常
	IP全体長	正常
	フラグメント	正常
TCP	TCPヘッダ長	正常
HTTP	リクエスト形式	違反

(b)

アクセスポリシー違反検知モジュール	チェック項目	チェック結果
I P	宛先アドレス	正常
	送信元アドレス	正常
TCP	宛先ポート	正常
	送信元ポート	正常
HTTP	URL内容	違反

(72)

( 5B089 GA11 GA21 GB02 HA03 HA06  
HA10 JA22 JA31 JB22 KA17  
KB04 KB06 KB13

(72)

5K030 GA15 HB16 HB18 HC01 KA04  
KA13 LA08 LB02 LD19 LD20  
9A001 CC06 JJ14 JJ25 LL03